RECEIVED
CENTRAL FAX CENTER
JUN 08 2011

REMARKS

Examiner rejected claims 1-21 under 35 U.S.C. §103 as being unpatentable over Figs. 1 and 2 of Applicant's admitted prior art (AAPA) and in view of U.S. Pat. Appl. Pub. Nos. 20080043686 (Sperti et al.) and 20050213553 (Wang).

With regard to claims 1 and 2, Examiner said that the AAPA discloses a rogue access point and transmit channel preprocessor. It does not. The AAPA only discloses a rogue access point preprocessor and not a preprocessor concerning transmit channel as does Applicant. Applicant's RogueAPTransmitChannel preprocessor detects a channel on which a received packet is transmitted. The AAPA does not do this. Therefore, the AAPA does not disclose Applicant's RogueAPTransmitChannel preprocessor and, therefore, does not disclose Applicant's claim 1 or claim 2.

Examiner said that Sperti et al., in paras. 74 and 128, and Wang, in para. 35, disclose Applicant's preprocessors as follows: RogueClient, BridgedNetwork, RogueClientValidAP, ValidClientRogueAP, AdhocNetwork, WrongChannel, CloakingViolation, EncryptionViolation, and NullSSIDViolation.

Examiner citation to Sperti et al. in paragraph 128 lists a configuration list of valid APs, clients, and channels. None of these disclose Applicant's preprocessors.

Examiner's citation to Sperti et al. in paragraph 128 also mentions that "an alert is generated when information obtained from a packet does not match the information in the configuration file." Such a citation is a broad description that discloses the general operation of an Intrusion Detection System such as SNORT, which Applicant admitted is prior art. Applicant did not claim to have invented the general operation of an IDS. Instead, Applicant claimed to have improved an IDS by including preprocessors that previously did not exist. Examiner's citation does not disclose the new preprocessors that Applicant included in Applicant's patent application.

Applicant's RogueClient preprocessor detects a rogue client. Nowhere in Examiner's citations is a preprocessor disclosed to detect a rogue client. Therefore, neither Sperti et al. nor Wang disclose Applicant's RogueClient preprocessor and, therefore, do not disclose Applicant's claim 1 or claim 2.

Applicant's BridgedNetwork preprocessor detects a wireless distribution system (or bridged network). Nowhere in Examiner's citations is a preprocessor disclosed to detect a wireless distribution system (or bridged network). Therefore, neither Sperti et al. nor Wang disclose Applicant's BridgedNetwork preprocessor and, therefore, do not disclose Applicant's claim 1 or claim 2.

Applicant's RogueClientValidAP preprocessor detects an unauthorized client attempting to connect to a valid access point (AP). Nowhere in Examiner's citations is a preprocessor disclosed to detect an unauthorized client attempting to connect to a valid AP. Therefore, neither Sperti et al. nor Wang disclose Applicant's RogueClientValidAP preprocessor and, therefore, do not disclose Applicant's claim 1 or claim 2.

Applicant's ValidClientRogueAP preprocessor detects an authorized client attempting to connect to a rogue AP. Nowhere in Examiner's citations is a preprocessor disclosed to detect an authorized client attempting to connect to a rogue AP. Therefore, neither Sperti et al. nor Wang disclose Applicant's ValidClientRogueAP preprocessor and, therefore, do not disclose Applicant's claim 1 or claim 2.

Applicant's AdhocNetwork preprocessor detects beacons for an ad-hoc network, two devices in an ad-hoc network, and an authorized client in ad-hoc mode with a rogue client. Nowhere in Examiner's citations is a preprocessor disclosed to detect beacons for an ad-hoc network, two devices in an ad-hoc network, and an authorized client in ad-hoc mode with a rogue client. Examiner's citation to Sperti et al. in paragraph 74 also mentions "RF Jamming using ad-hoc networks." Using an ad-hoc network does not disclose Applicant's AdHocNetwork preprocessor, because using an ad-hoc network does not disclose detecting beacons for an ad-hoc network, two devices in an ad-hoc network, and an authorized client in ad-hoc mode with a rogue

client as does Applicant's AdHocNetwork preprocessor. Therefore, Examiner's citations do not disclose Applicant's AdHocNetwork preprocessor. Therefore, neither Sperti et al. nor Wang disclose Applicant's AdHocNetwork preprocessor and, therefore, do not disclose Applicant's claim 1 or claim 2.

Applicant's WrongChannel preprocessor detects a device operating on an unauthorized channel. Nowhere in Examiner's citations is a preprocessor disclosed to detect a device operating on an unauthorized channel. Therefore, neither Sperti et al. nor Wang disclose Applicant's WrongChannel preprocessor and, therefore, do not disclose Applicant's claim 1 or claim 2.

Applicant's CloakingViolation preprocessor detects when an SSID is not NULL when it should be NULL. Nowhere in Examiner's citations is a preprocessor disclosed to detect when an SSID is not NULL when it should be NULL. Therefore, neither Sperti et al. nor Wang disclose Applicant's CloakingViolation preprocessor and, therefore, do not disclose Applicant's claim 1 or claim 2.

Applicant's EncryptionViolation preprocessor detects when a device is operating counter to an encryption policy (i.e., not using encryption when the policy requires encryption and using encryption when the policy requires no encryption). Nowhere in Examiner's citations is a preprocessor disclosed to detect when a device is operating counter to an encryption policy. Examiner's citation to Sperti et al. in paragraph 128 also mentions "authentication and encryption method." Examiner failed to put the citation in proper context. The actual citation is to "encryption and authentication method used." So, examiner's citation is to using an encryption method. Using an encryption method is not the same as detecting if a device is violating an encryption policy as does Applicant's EncryptionViolation preprocessor. Therefore, Examiner's citation does not disclose Applicant's EncryptionViolation preprocessor.
Therefore, neither Sperti et al. nor Wang disclose Applicant's EncryptionViolation preprocessor and, therefore, do not disclose Applicant's claim 1 or claim 2.

Applicant's NullSSIDViolation preprocessor detects when a device attempts to associate with a client that sent a NULL SSID. Nowhere in Examiner's citations is a preprocessor disclosed to detect when a device attempts to associate with a client that sent a NULL SSID. Examiner said that Wang, in paragraph 35, discloses detecting attacks related to cloaking violations and NULL SSID. Examiner appears to quote Wang as disclosing "detecting attacks comprising a NULL/weak/default SSID probe request sent to an AP in an association or re-association request in an attempt to violate the cloaking policy of "cloaking or defaulting" the SSID of an AP." If this was intended to be a quote, it was mistakenly quoted, because the citation neven discloses the use of a NULL SSID. Instead, an SSID is checked to determine if it is weak or is a default SSID. Neither a weak nor a default SSID is a NULL SSID. Per the two attachment documents from About.com, a default SSID is a defined SSID set by the manufacturer of the device. A weak SSID implies that it is an SSID that is easily determined. A NULL SSID is no SSID, which is neither a defined SSID nor an easily determined SSID. In addition, Examiner's citation never mentions NULL. The Examiner inserted NULL himself. Examiner appears to have improperly used Applicant's application as the motivation to insert NULL into a citation that did not include NULL. Examiner committed error by doing so. Furthermore, Examiner associates "defaulting" with "cloaking". "Cloaking is the use of a NULL SSID, whereas "defaulting" is the setting of an SSID to a default value. "defaulting" is not equivalent to "cloaking." Therefore, Examiner committed error by associating the terms. Therefore, neither Sperti et al. nor Wang disclose Applicant's NULLSSIDViolation preprocessor and, therefore, do not disclose Applicant's claim 1 or claim 2.

Examiner said that it would be obvious to one of ordinary skill to modify the teachings of the AAPA to include preprocessors for detecting attacks taught by Sperti and Wang for the purpose of increased security by having a system that can detect as many attacks as possible. Examiner admits that Sperti et al. and Wang was not cited for disclosing Applicant's preprocessors but for disclosing attacks. An attack is not a preprocessor, because there may be many different solutions to an attack. A preprocessor is a specific solution to an attack.

Therefore, an attack cannot and does not disclose the specific preprocessors disclosed by Applicant. Sperti et al. and Wang do not disclose Applicant's preprocessors and, therefore, do not disclose Applicant's claim 1 or claim 2.

With regard to claims 3 and 13, Examiner said that the combination of the AAPA, Sperti et al. and Wang disclose claim 2. For the reasons given above, the combination of the AAPA, Sperti et al. and Wang do not disclose claim 2. However, it appears that Examiner meant to say claim 3. So, Applicant responds below assuming that Examiner meant claim 3.

Examiner appears to have meant to say that the AAPA, Sperti in paragraphs 73-81, 105-106, and 130-166 disclose Applicant's claims 3 and 13. Examiner's citation to the AAPA is to a description of the SNORT intrusion detection system. SNORT does not include a RogueAPTransmitChannel preprocessor of Applicant's invention and does not disclose any of the steps of claims 3 and 13. Examiner's citation to Sperti et al. is to a description of a detection module device, a configuration module device, and a list of attacks, including a DEAUTH attack, a LEAP attack, RF jamming, Denial of Service, man in the middle, fake access point, WEP cracking, injection of spurious traffic, and NETSTUMBLER. The two examples Examiner cited are to attacks that Applicant does not claim in claims 3 and 13. In addition, claims 3 and 13 includes all of the limitations of claim 2 and claims 2-3, respectively, which, for the reasons given above, Sperti does not disclose. Applicant's claims 3 and 13 are methods of performing Applicant's rogue access point and transmit channel preprocessor. Since the combination of the AAPA and Sperti et al. does not include all of the steps of claims 3 and 13, the combination of the AAPA and Sperti et al. does not disclose claims 3 and 13.

The first step of claims 3 and 13 is determining a frame type of the packet. Nowhere in Examiner's citations is such a step disclosed.

The second step of claims 3 and 13 is determining if the frame type contains a basic service set identifier (BSSID) or is an acknowledgement message (ACK). Nowhere in Examiner's citations is such a step disclosed.

The third step of claims 3 and 13 is if the frame does not contain a BSSID and is not an ACK then setting global variable Transmit_Channel equal to zero and returning to step (h) in claim 2. Nowhere in Examiner's citations is such a step disclosed.

The fourth step of claims 3 and 13 is if the frame contains a BSSID or is an ACK then determining if the packet is a beacon frame or a probe response. Nowhere in Examiner's citations is such a step disclosed.

The fifth step of claims 3 and 13 is if either frame type is identified then identifying the BSSID and the channel in its header. Nowhere in Examiner's citations is such a step disclosed.

The sixth step of claims 3 and 13 is determining if the BSSID is in a rogue AP list. Nowhere in Examiner's citations is such a step disclosed.

The seventh step of claims 3 and 13 is if the BSSID is not in the rogue AP list then determining if the BSSID is on a valid AP list. Nowhere in Examiner's citations is such a step disclosed.

The eighth step of claims 3 and 13 is if the BSSID is not on the valid AP list then adding the BSSID and its channel to the rogue AP list, setting global variable Transmit_Channel equal to the BSSID channel, and returning to step (h) in claim 2. Nowhere in Examiner's citations is such a step disclosed.

The ninth step of claims 3 and 13 is if the BSSID is in the rogue AP list or the BSSID is not in the rogue AP list but is in the valid AP list then updating the channel information in the corresponding rogue and valid AP list entry, setting global variable Transmit_Channel equal to the BSSID channel, and returning to step (h) in claim 2. Nowhere in Examiner's citations is such a step disclosed.

The tenth step of claims 3 and 13 is if the frame is neither a beacon frame nor a probe response then finding the BSSID in the header. Nowhere in Examiner's citations is such a step disclosed.

The eleventh step of claims 3 and 13 is determining if the BSSID or destination address is in a rogue AP list. Nowhere in Examiner's citations is such a step disclosed.

The twelfth step of claims 3 and 13 is if the BSSID or the destination address are in the rogue AP list then determining its channel in the rogue AP list, setting global variable Transmit_Channel equal to the BSSID channel, and returning to step (h) in claim 2. Nowhere in Examiner's citations is such a step disclosed.

The thirteenth step of claims 3 and 13 is if the BSSID and the destination address are not in the rogue AP list then determining if the BSSID or destination address are on the valid AP list. Nowhere in Examiner's citations is such a step disclosed.

The fourteenth step of claims 3 and 13 is if the BSSID and the destination address are on the valid AP list then determining the BSSID channel in the valid AP list, setting the global variable Transmit_Channel equal to the BSSID channel, and returning to step (h) in claim 2. Nowhere in Examiner's citations is such a step disclosed.

The fifteenth step of claims 3 and 13 is if the BSSID and the destination address are not on the valid AP list then adding the BSSID to the rogue AP list with channel equal to zero, setting the global variable Transmit_Channel equal to zero, and returning to step (h) in claim 2. Nowhere in Examiner's citations is such a step disclosed.

Examiner said that the AAPA, Sperti in paragraphs 73-81, 105-106, and 130-166, and Wang disclose Applicant's claim 4. Examiner did not cite anything specific in the AAPA or Wang, but only cited specifics from Sperti et al. Examiner's citation to Sperti et al. is to a description of a detection module device, a configuration module device, and a list of attacks, including a DEAUTH attack, a LEAP attack, RF jamming, Denial of Service, man in the middle, fake access point, WEP cracking, injection of spurious traffic, and NETSTUMBLER. The two examples Examiner cited are to attacks that Applicant does not claim in claim 4. In addition, claim 4 includes all of the limitations of claim 2 which, for the reasons given above, Sperti does not disclose. Applicant's claim 4 is a method of preprocessing a packet using a rogue client preprocessor as follows.

The first step of claim 4 is determining a frame type of the packet. Nowhere in Examiner's citations is such a step disclosed.

The second step of claim 4 is determining if the frame type contains a source address. Nowhere in Examiner's citations is such a step disclosed.

The third step of claim 4 is if the frame type does not contain a source address then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The fourth step of claim 4 is if the frame contains a source address then finding the source address in its header. Nowhere in Examiner's citations is such a step disclosed.

The fifth step of claim 4 is determining if the packet is from an access point. Nowhere in Examiner's citations is such a step disclosed.

The sixth step of claim 4 is if the packet is from an access point then returning to step (h) in claim 2. Nowhere in Examiner's citations is such a step disclosed.

The seventh step of claim 4 is determining if the source address is in a rogue client list. Nowhere in Examiner's citations is such a step disclosed.

The eighth step of claim 4 is if the source address is not on the rogue client list then determining if the source address is on a valid client list. Nowhere in Examiner's citations is such a step disclosed.

The ninth step of claim 4 is if the source address is on the valid client list then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The tenth step of claim 4 is if the packet is not on the valid client list then adding the source address to the rogue client list, generating an alert message to indicate that a rogue client has been detected, and returning to step (h) in claim 2. Nowhere in Examiner's citations is such a step disclosed.

The eleventh step of claim 4 is if the source address is on the rogue client list then determining if a user-defined time period has expired. Nowhere in Examiner's citations is such a step disclosed.

The twelfth step of claim 4 is if the user-definable time-period has not expired then returning to step (h) in claim 2. Nowhere in Examiner's citations is such a step disclosed.

The thirteenth step of claim 4 is if the user-definable time-period has expired then adding the source address to the rogue client list, generating an alert message to indicate that a rogue client had been detected, and returning to step (h) in claim 2. Nowhere in Examiner's citations is such a step disclosed.

Examiner said that the AAPA, Wang, and Sperti in paragraphs 73-81, 105-106, and 130-166 disclose Applicant's claims 5 and 14. Examiner did not cite anything specific in the AAPA or Wang, but only cited specifics from Sperti et al. Examiner's citation to Sperti et al. is to a description of a detection module device, a configuration module device, and a list of attacks, including a DEAUTH attack, a LEAP attack, RF jamming, Denial of Service, man in the middle, fake access point, WEP cracking, injection of spurious traffic, and NETSTUMBLER. The two examples Examiner cited are to attacks that Applicant does not claim in either claim 5 or claim 14. In addition, claim 14 includes all of the limitations of claims 3 and 13 which, for the reasons given above, Sperti does not disclose. Applicant's claims 5 and 14 are methods of preprocessing a packet using a bridged network preprocessor as follows.

The first step of claims 5 and 14 is finding a frame type of the packet. Nowhere in Examiner's citations is such a step disclosed.

The second step of claims 5 and 14 is determining if the frame contains a source address. Nowhere in Examiner's citations is such a step disclosed.

The third step of claims 5 and 14 is if the frame type does not contain a source address then returning to step (h) in claim 2. Nowhere in Examiner's citations is such a step disclosed.

The fourth step of claims 5 and 14 is if the frame contains a source address then determining if the frame is a data frame. Nowhere in Examiner's citations is such a step disclosed.

The fifth step of claims 5 and 14 is if the frame is not a data frame then returning to step (h) in claim 2. Nowhere in Examiner's citations is such a step disclosed.

The sixth step of claims 5 and 14 is if the frame is a data frame then determining if to_ds and from_ds are each set to one. Nowhere in Examiner's citation is such a step disclosed.

The seventh step of claims 5 and 14 is if to_ds and from_ds are not both set to one then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The eighth step of claims 5 and 14 is if to_ds and from_ds are each set to one then determining if the source and destination addresses are on an alert list. Nowhere in Examiner's citation is such a step disclosed.

The ninth step of claims 5 and 14 is if the source and destination addresses are on the alert list then determining if a user-definable time-period has expired. Nowhere in Examiner's citation is such a step disclosed.

The tenth step of claims 5 and 14 is if the user-definable time-period has not expired then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The eleventh step of claims 5 and 14 is if either the user-definable time-period has expired or if the source and destination addresses are not on the alert list then adding the source and destination addresses to the alert list, generating an alert that indicates that a bridged network has been detected, and returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

Examiner said that the AAPA, Wang, and Sperti in paragraphs 73-81, 105-106, and 130-166 disclose Applicant's claims 6 and 15. Examiner did not cite anything specific in the AAPA or Wang, but only cited specifics from Sperti et al. Examiner's citation to Sperti et al. is to a description of a detection module device, a configuration module device, and a list of attacks, including a DEAUTH attack, a LEAP attack, RF jamming, Denial of Service, man in the middle, fake access point, WEP cracking, injection of spurious traffic, and NETSTUMBLER. The two examples Examiner cited are to attacks that Applicant does not claim in either claim 6 or claim 15. In addition, claim 15 includes all of the limitations of claims 3 and 13-14 which, for the reasons given above, Sperti does not disclose. Applicant's claims 6 and 15 are methods of preprocessing a packet using a rogue client valid access point preprocessor as follows.

The first step of claims 6 and 15 is finding a frame type of the packet. Nowhere in Examiner's citation is such a step disclosed.

The second step of claims 6 and 15 is determining if the frame contains a source address. Nowhere in Examiner's citation is such a step disclosed.

The third step of claims 6 and 15 is if the frame does not contain a source address then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The fourth step of claims 6 and 15 is if the frame contains a source address then determining if the frame is an authentication request. Nowhere in Examiner's citation is such a step disclosed.

The fifth step of claims 6 and 15 is if the frame is an authentication request then determining if the source address is on a rogue client list. Nowhere in Examiner's citation is such a step disclosed.

The sixth step of claims 6 and 15 is if the frame is not an authentication request then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The seventh step of claims 6 and 15 is if the source address is not on the rogue client list then determining if the source address is on the valid client list. Nowhere in Examiner's citation is such a step disclosed.

The eighth step of claims 6 and 15 is if the source address is on the valid client list then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The ninth step of claims 6 and 15 is if the source address is either on the rogue client list or not on the rogue client list or the valid client list then determining if the destination access point address is valid. Nowhere in Examiner's citation is such a step disclosed.

The tenth step of claims 6 and 15 is if the destination access point address is not valid then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The eleventh step of claims 6 and 15 is if the destination access point address is valid then determining if the source address is on a bad authentication request list. Nowhere in Examiner's citation is such a step disclosed.

The twelfth step of claims 6 and 15 is if the source address is on the bad authentication request list then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The thirteenth step of claims 6 and 15 is if the source address is not on the bad authentication request list then adding the source address to the bad authentication request list, generating an alert to indicate that an unauthorized client is attempting to connect to a valid access point, and returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

Examiner said that the AAPA, Wang, and Sperti in paragraphs 73-81, 105-106, and 130-166 disclose Applicant's claims 7 and 16. Examiner did not cite anything specific in the AAPA or Wang, but only cited specifics from Sperti et al. Examiner's citation to Sperti et al. is to a description of a detection module device, a configuration module device, and a list of attacks, including a DEAUTH attack, a LEAP attack, RF jamming, Denial of Service, man in the middle, fake access point, WEP cracking, injection of spurious traffic, and NETSTUMBLER. The two examples Examiner cited are to attacks that Applicant does not claim in either claim 7 or claim 16. In addition, claim 16 includes all of the limitations of claims 3 and 13-15 which, for the reasons given above, Sperti does not disclose. Applicant's claims 7 and 16 are methods of preprocessing a packet using valid client rogue access point preprocessor as follows.

The first step of claims 7 and 16 is determining a frame type of the packet. Nowhere in Examiner's citation is such a step disclosed.

The second step of claims 7 and 16 is determining if the frame contains a source address. Nowhere in Examiner's citation is such a step disclosed.

The third step of claims 7 and 16 is if the frame does not contain a source address then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The fourth step of claims 7 and 16 is if the frame contains a source address then determining if the frame is an authentication request. Nowhere in Examiner's citation is such a step disclosed.

The fifth step of claims 7 and 16 is if the frame is not an authentication request then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The sixth step of claims 7 and 16 is if the frame is an authentication request then determining if the source address is on a rogue client list. Nowhere in Examiner's citation is such a step disclosed.

The seventh step of claims 7 and 16 is if the source address is on a rogue client address then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The eighth step of claims 7 and 16 is if the source address is not on a rogue client address then determining if the source address is on a valid client list. Nowhere in Examiner's citation is such a step disclosed.

The ninth step of claims 7 and 16 is if the source address is not on the valid client list then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The tenth step of claims 7 and 16 is if the source address is on the valid client list then determining if the destination address is rogue. Nowhere in Examiner's citation is such a step disclosed.

The eleventh step of claims 7 and 16 is if the destination address is not rogue then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The twelfth step of claims 7 and 16 is if the destination address is rogue then determining if the source address is on a bad authentication request list. Nowhere in Examiner's citation is such a step disclosed.

The thirteenth step of claims 7 and 16 is if the source address is on a bad authentication request list then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The fourteenth step of claims 7 and 16 is if the source address is not on the bad authentication request list then adding the source address to the bad authentication request list, generating an alert to indicate that an authorized client is attempting to connect to a rogue access point, and returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

Examiner said that the AAPA, Wang, and Sperti in paragraphs 73-81, 105-106, and 130-166 disclose Applicant's claims 8 and 17. Examiner did not cite anything specific in the AAPA or Wang, but only cited specifics from Sperti et al. Examiner's citation to Sperti et al. is to a description of a detection module device, a configuration module device, and a list of attacks, including a DEAUTH attack, a LEAP attack, RF jamming, Denial of Service, man in the middle, fake access point, WEP cracking, injection of spurious traffic, and NETSTUMBLER. The two examples Examiner cited are to attacks that Applicant does not claim in either claim 8 or claim 17. In addition, claim 17 includes all of the limitations of claims 3 and 13-16 which, for the reasons given above, Sperti does not disclose. Applicant's claims 8 and 17 are methods of preprocessing a packet using an ad-hoc network preprocessor as follows.

The first step of claims 8 and 17 is determining a frame type of the packet. Nowhere in Examiner's citation is such a step disclosed.

The second step of claims 8 and 17 is determining if the frame contains a source address. Nowhere in Examiner's citation is such a step disclosed.

The third step of claims 8 and 17 is if the frame does not contain a source address then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The fourth step of claims 8 and 17 is if the frame contains a source address then determining if the frame is a beacon or a probe response. Nowhere in Examiner's citation is such a step disclosed.

The fifth step of claims 8 and 17 is if the frame is a beacon or probe response then determining if ESS is equal to zero and IBSS is equal to one. Nowhere in Examiner's citation is such a step disclosed.

The sixth step of claims 8 and 17 is if ESS is not equal to zero or IBSS is not equal to one then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The seventh step of claims 8 and 17 is if ESS is equal to zero and IBSS is equal to one then adding the source address to the ad-hoc beacon alert list, generating an ad-hoc beacon detected alert, and returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The eighth step of claims 8 and 17 is if the frame is neither a beacon nor a probe request then determining if the frame is a data frame. Nowhere in Examiner's citation is such a step disclosed.

The ninth step of claims 8 and 17 is if the frame is not a data frame then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The tenth step of claims 8 and 17 is if the frame is a data frame then determining if to_ds and from_ds are each set to zero. Nowhere in Examiner's citation is such a step disclosed.

The eleventh step of claims 8 and 17 is if to_ds and from_ds are not both set to zero then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The twelfth step of claims 8 and 17 is if to_ds and from_ds are each set to zero then determining if the source and destination addresses are on an active ad-hoc network alert list. Nowhere in Examiner's citation is such a step disclosed.

The thirteenth step of claims 8 and 17 is if the source and destination addresses are on the active ad-hoc network alert list then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The fourteenth step of claims 8 and 17 is if the source and destination addresses are not on the active ad-hoc network alert list then adding the source and destination addresses to the alert list and generating an active ad-hoc network detected alert. Nowhere in Examiner's citation is such a step disclosed.

The fifteenth step of claims 8 and 17 is determining if the source address is on a valid client list. Nowhere in Examiner's citation is such a step disclosed.

The sixteenth step of claims 8 and 17 is if the source address is not on the valid client list then determining if the destination address is on the valid client list. Nowhere in Examiner's citation is such a step disclosed.

The seventeenth step of claims 8 and 17 is if the destination address is not on the valid client list then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The eighteenth step of claims 8 and 17 is if the destination address is on the valid client list then generating an authorized client in ad-hoc conversation with rogue client alert, and returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The nineteenth step of claims 8 and 17 is if the source address is on the valid client list then determining if the destination address is on the valid client list. Nowhere in Examiner's citation is such a step disclosed.

The twentieth step of claims 8 and 17 is if the destination address is not on the valid client list then generating an authorized client in ad-hoc conversation with rogue client alert, and returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The twenty-first step of claims 8 and 17 is if the destination address is on the valid client list then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

Examiner said that the AAPA, Wang, and Sperti in paragraphs 73-81, 105-106, and 130-166 disclose Applicant's claims 9 and 18. Examiner did not cite anything specific in the AAPA or Wang, but only cited specifics from Sperti et al. Examiner's citation to Sperti et al. is to a description of a detection module device, a configuration module device, and a list of attacks, including a DEAUTH attack, a LEAP attack, RF jamming, Denial of Service, man in the middle, fake access point, WEP cracking, injection of spurious traffic, and NETSTUMBLER. The two examples Examiner cited are to attacks that Applicant does not claim in either claim 9 or claim 18. In addition, claim 18 includes all of the limitations of claims 3 and 13-17 which, for the reasons given above, Sperti does not disclose. Applicant's claims 9 and 18 are methods of preprocessing a packet using a wrong channel preprocessor as follows.

The first step of claims 9 and 18 is determining a frame type of the packet. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 9 and 18 is determining if the frame contains a source address. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 9 and 18 is if the frame does not contain a source address then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 9 and 18 is if the frame contains a source address then determining the source address in its header. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 9 and 18 is determining if the source address is in a valid client list. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 9 and 18 is if the source address is not in the valid client list then determining if the source address is in a valid access point list. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 9 and 18 is if the source address is not in the valid access point list then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 9 and 18 is if the source address is in the valid client list or not in the valid client list but in the valid access point list then determining and recording the designated operating channel. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 9 and 18 is determining if the source address is in a wrong channel alert list. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 9 and 18 is if the source address is in the wrong channel alert list then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 9 and 18 is if the source address is not in the wrong channel alert list then determining if a transmit channel on which the packet was transmitted is a designated operating channel for the source address. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 9 and 18 is if the transmit channel is equal to the designated operating channel then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 9 and 18 is if the transmit channel is not equal to the designated operating channel then adding the source address to the wrong channel alert list, generating a device operating on the wrong channel alert, and returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

Examiner said that the AAPA, Wang, and Sperti in paragraphs 73-81, 105-106, and 130-166 disclose Applicant's claims 10 and 19. Examiner did not cite anything specific in the AAPA or Wang, but only cited specifics from Sperti et al. Examiner's citation to Sperti et al. is to a description of a detection module device, a configuration module device, and a list of attacks, including a DEAUTH attack, a LEAP attack, RF jamming, Denial of Service, man in the middle, fake access point, WEP cracking, injection of spurious traffic, and NETSTUMBLER. The two examples Examiner cited are to attacks that Applicant does not claim in either claim 10 or claim 19. In addition, claim 19 includes all of the limitations of claims 3 and 13-18 which, for the reasons given above, Sperti does not disclose. Applicant's claims 10 and 19 are methods of preprocessing a packet using a cloaking violation preprocessor as follows.

The first step of claims 10 and 19 is determining a frame type of the packet. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 10 and 19 is determining if the frame is a beacon. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 10 and 19 is if the frame is not a beacon then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 10 and 19 is if the frame is a beacon then determining if cloaking_required is equal to a one. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 10 and 19 is if cloaking_required is not equal to a one then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 10 and 19 is if cloaking_required is equal to a one then determining if SSID is null. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 10 and 19 is if SSID is null then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 10 and 19 is if SSID is not null then determining if the source address of the packet is on a cloaking policy alert list. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 10 and 19 is if the source address of the packet is on the cloaking policy alert list then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 10 and 19 is if the source address of the packet is not on the cloaking policy alert list then adding the source address to the cloaking policy alert list, generating a SSID cloaking policy violation detected alert, and returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

Examiner said that the AAPA, Wang, and Sperti in paragraphs 73-81, 105-106, and 130-166 disclose Applicant's claims 11 and 20. Examiner did not cite anything specific in the AAPA or Wang, but only cited specifics from Sperti et al. Examiner's citation to Sperti et al. is to a description of a detection module device, a configuration module device, and a list of attacks, including a DEAUTH attack, a LEAP attack, RF jamming, Denial of Service, man in the middle, fake access point, WEP cracking, injection of spurious traffic, and NETSTUMBLER. The two examples Examiner cited are to attacks that Applicant does not claim in either claim 11 or claim 20. In addition, claim 20 includes all of the limitations of claims 3 and 13-19 which, for the reasons given above, Sperti does not disclose. Applicant's claims 11 and 20 are methods of preprocessing a packet using an encryption violation preprocessor as follows.

The first step of claims 11 and 20 is determining a frame type of the packet. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 11 and 20 is determining if the frame is a probe response or a beacon frame. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 11 and 20 is if the frame is neither a probe response nor a beacon frame then determining if the frame is a data frame or an authentication frame. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 11 and 20 is if the frame is neither a data frame nor an authentication frame then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 11 and 20 is if the frame is a probe response, beacon frame, data frame, or authentication frame then determining if encryption_required is set to a one. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 11 and 20 is if encryption_required is not set to a one then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 11 and 20 is if encryption_required is set to a one and the frame is a data frame or an authentication frame then determining if wep is a one. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 11 and 20 is if wep is a one then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 11 and 20 is if wep is not a one then determining if the source address of the packet is on an encryption policy alert list. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 11 and 20 is if the source address of the packet is on the encryption policy alert list then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 11 and 20 is if the source address of the packet is not on the encryption policy alert list then adding the source address to the encryption policy alert list,

generating an encryption policy violation detection alert, and returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 11 and 20 is if encryption_required is set to a one and the frame is a beacon or a probe response frame then determining if a privacy field is set to a one. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 11 and 20 is if the privacy field is set to a one then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 11 and 20 is if the privacy field is not set to a one then determining if the source address is on the encryption policy alert list. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 11 and 20 is if the source address is on the encryption policy alert list then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 11 and 20 is if the source address is not on the encryption policy alert list then adding the source address to the encryption policy alert list, generating an encryption policy violation detection alert, and returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

Examiner said that the AAPA, Wang, and Sperti in paragraphs 73-81, 105-106, and 130-166 disclose Applicant's claims 12 and 21. Examiner did not cite anything specific in the AAPA or Wang, but only cited specifics from Sperti et al. Examiner's citation to Sperti et al. is to a description of a detection module device, a configuration module device, and a list of attacks, including a DEAUTH attack, a LEAP attack, RF jamming, Denial of Service, man in the middle, fake access point, WEP cracking, injection of spurious traffic, and NETSTUMBLER. The two examples Examiner cited are to attacks that Applicant does not claim in either claim 12 or claim 21. In addition, claim 21 includes all of the limitations of claims 3 and 13-20 which, for the reasons given above, Sperti does not disclose. Applicant's claims 12 and 21 are methods of preprocessing a packet using a null SSID violation preprocessor as follows.

The first step of claims 12 and 21 is determining a frame type of the packet. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is determining if the frame is a probe request. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if the frame is a probe request then determining if null_ssid_assoc is set to a zero. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21, as amended, is if null_ssid_assoc is not set to a zero then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if null_ssid_assoc is set to a zero then determining if SSID is null. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if SSID is not null then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if SSID is set to null then determining if the source address of the packet is in a broadcast probe request senders list. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if the source address of the packet is in the broadcast probe request senders list then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if the source address of the packet is not in the broadcast probe request senders list then adding the source address to the broadcast probe request senders list and returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if the frame is not a probe request then determining if the frame is a probe response. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if the frame is a probe response then determining a destination address in its header. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is determining if the destination address is in the broadcast probe request senders list. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if the destination address is not in the broadcast probe request senders list then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if the destination address is on the broadcast probe request senders list then determining if the source address is on a broadcast probe alert list. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if the source address is on the broadcast probe alert list then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if the source address is not on the broadcast probe alert list then adding the source address to the broadcast probe alert list, generating a Null SSID association alert, and returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if the frame is not a probe response then determining if the frame is an association request. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if the frame is an association request then determining if null_ssid_assoc is set to a zero. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if null_ssid_assoc is not set to a zero then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if null_ssid_assoc is set to a zero then determining if SSID is set to null. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21, as amended, is if SSID is not set to null then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if SSID is set to null then determining if the source address is on a broadcast association request senders list. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if the source address is on the broadcast association request senders list then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if the source address is not on the broadcast association request senders list then adding the source address to the broadcast association request senders list, and returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if the frame is not an association request then determining if the frame is an association response. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if the frame is not an association response then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if the frame is an association response then determining a destination address in its header. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is determining if the destination address is on the broadcast association request senders list. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if the destination address is not on the broadcast association request senders list then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if the destination address is on the broadcast association request senders list then determining if the source address is on a broadcast association alert list. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if the source address is on the broadcast association alert list then returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

The first step of claims 12 and 21 is if the source address is not on the broadcast association alert list then adding the source address to the broadcast association alert list, generating a Null SSID association alert, and returning to step (h) in claim 2. Nowhere in Examiner's citation is such a step disclosed.

For the reasons given above, Applicant rebuts Examiner's obviousness rejection of claim 1-21. Applicant submits that the application is in condition for allowance.

Reconsideration of the application in light of the rebuttal is requested. Allowance of claims 1-21 is solicited.

Respectfully submitted,

Robert D. Morelli
Registration No. 37,398
(301) 688-0287